## Claims

1-5. (Cancelled)

6. (Currently Amended) A cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including ~~at least two processing units~~ a first processing unit and a second processing unit configured to determine a Montgomery product of the cryptographic parameters, the first processing unit and the second processing unit ~~each processing unit receiving~~ configured to receive a first bit and a second bit ~~a bit~~ corresponding to the first parameter, respectively, and partial words of the second parameter.

7. (Currently Amended) The processor of claim 6, wherein the first ~~at least one~~ processing unit is configured to communicate intermediate values of partial words of the Montgomery product to ~~a different~~ the second processing unit.

8. (Previously Presented) The processor of claim 6, further comprising a field-type input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic, wherein $GF(p)$ is a prime field, $GF(2^m)$ is a binary extension field, $p$ is a positive prime number, and $m$ is a positive integer.

9. (Previously Presented) The processor of claim 8, wherein the arithmetic operation selectable with the field-type input is field addition.

10. (Previously Presented) The processor of claim 8, further comprising a dual-field adder in communication with the field-type input.

11. (Previously Presented) The processor of claim 10, wherein the first and second cryptographic parameters are represented as $m$ bits and $e$ words of word length $w$, wherein $e = \lceil (m+1)/w \rceil$, and $m$, $e$, and $w$ are positive integers.

12-15. (Cancelled)

16. (Currently Amended) A method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits;

representing the second cryptographic parameter and a modulus as a series of words;

processing a first bit of the first parameter with each word of the modulus and each word of the second parameter to produce a first series of intermediate values and a contribution to the Montgomery product based on the first bit;

processing a second bit of the first parameter with each word of the modulus and each word of the second parameter, and a corresponding intermediate value from the first series of intermediate values to produce a second series of intermediate values and a contribution to the Montgomery product based on the second bit;

~~determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage;~~

~~determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage;~~ and

combining the ~~intermediate values~~ first contribution and the second contribution ~~to form the Montgomery product of the first cryptographic parameter and the second cryptographic parameter~~.

17. (Previously Presented) The method of claim 16, further comprising determining intermediate values based on a field-type input that selects an addition operation corresponding to addition with carry or without carry.

18. (original) A computer-readable medium containing instructions for executing the method of claim 17.

19-21. (Cancelled)

22. (New) The cryptographic processor of claim 6, wherein the multiplication module further comprise a third processing unit and a fourth processing unit configured to receive a third

bit and a fourth bit, respectively, corresponding to the first parameter and partial words of the second parameter.